View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Texas A&M Repository

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Managing the Risk of Organizational Incidents

Brian R. Dickson
Dept. Chemical & Process Engineering
University of Strathclyde, Glasgow, G1 1XJ, UK.
Email: brian.dickson@strath.ac.uk

Key Words: Process Safety Management, Risk, Human factors

Abstract

In Reason's, *Managing the Risk of Organizational Incidents,* `Reason draws on the work of other authors, and how awareness of the operating consequences of action is more important that causes of error.
It is the intention of this paper to review some of this work, in particular in the light of current trends that promote Risk Management, Incident Recording and Lead/Lagging Indicators as the "new direction in safety management". It will then go on to suggest why we need to encompass more of general management principles in the way that we think about safety in the work place and perhaps create new tools that move away from the Engineering model and its linear solutions, to an Organizational Model, where responsibility lies with the Individual rather than the System.

It will draw on case studies to demonstrate a sample of how the approach may have validity.

Introduction

In 2016, I asked a Masters Chemical Engineering student to consider major process safety events over the past 25 years, to consider whether there were common patterns across 20+ incidents by applying principles from good audit practice set. We hoped to then factorise these against frequency and build a model of a predictive nature.

What we discover was that the influencing factors could be set out into design, safety processes, management practice, legislator demands, Safety models, current development or trends.

As part of this work, we set out Stages in Safety Practice (SP) as follows:

1. F (Materials of Construction (M_c), Property of Materials (P_m), Reaction Kinetics (R_k), Effect of Fires & Explosions (E_{fe})),

2. HAZOP (H_z), LOPA (L_{pa})

3. Safety Case/COMAH (S_c), QRA(Q_{ra}),

4. Management of Change (M_{ch}), Swiss Cheese Model (S_{cm}) and Safety Management Systems (SMS)

5. Leading/Lagging Indicators (L_{li}), Stress Cracking (S_{cr}), Management of Safety Competence (M_{sc})

This could be written in a quasi-Equation of State as;

$$SP = F\,[M_{c,}\ P_{m,}\ R_{k,}\ E_{fe,}\ H_{z,}\ L_{pa,}\ S_c,\ Q_{ra,}\ M_{ch,}\ S_{cm,}\ Lli_{,}\ S_{cr,}\ M_{sc}\ ]$$

and my source of reference: Perry, Lees, CCPS (Eng. Design for Process Safety) Kletz (What went wrong), IChemE (Hazop), Reason (Human Factors), CCPS (Implementing Process Safety Management System), CCPS (Integrating Management Systems & Metrics to improve Process Safety Performance) and 30 other books on my shelf **but lastly Dekker [2] (Drift into Failure)**

It was perhaps now impossible to codify as we had thought because of the many factors involved, and had to rethink out linear simple engineering tool approach.

Yet on re-reading Dekker and Reason, we arrived at a tentative link between **Management of Safety Competence (M_{sc}), Safety Space and Drift into Failure.**

Discussion

To understand why there is perhaps a theory with considering, it’s worth considering some of the writings on the causes of what is often referred to as an Atrophy of Progress and the lessons that need to be drawn.

Charles Perrow [3], an organizational theorist, suggests a bleak proposition that “accidents are inevitable in complex, tightly-coupled systems ……...regardless of the skills of their operators and managers.”

Hence the title: accidents in such systems are 'normal'" According to Perrow the redundancies that go to make up defences-in-depth have three dangerous features.

1. Redundant defensive back-ups increase the interactive complexity of high-technology organizations and thus increase the likelihood of unforeseeable common-mode failures. While the assumption of independence may be appropriate for purely technical breakdowns, human errors at the 'sharp end', in the maintenance sector and in the managerial domains are uniquely capable of creating failures that can affect a number of defensive layers simultaneously"
2. Addin**g** redundancy makes the system more opaque to the p**e**ople who nominally control and manage it. Undiscovered errors and other latent problems accumulate over time and increase the likelihood of the 'holes' in the defensive lining up to permit the passage of an accident trajectory. This alignment of the gaps can be created either by interactive common-mode failures or by the simultaneous disabling of supposedly independent defences, as at Chernobyl.
3. As a consequence of this dangerous concealment, and because their obvious engineering sophistication, redundant defences can cause systems operators and managers to forget to be afraid. This false sense of security prompts them to strive even higher levels of production. Fixes including safety devices, often merely allow those in charge to run the system faster, or… with bigger explosives”

Karl Weick reinforces this view of unstable systems in control and tells us that “We know that single causes are rare, but we don't know how small events can become chained together so that they result in a disastrous outcome. In the absence of this understanding, people must wait until some crisis actually occurs before they can diagnose a problem, rather than be in a position to detect a potential problem before it emerges.

To anticipate and forestall disasters is to understand regularities in the ways small events can combine to have disproportionately large effects.” [4]

In taking forward this view, we appear to set ourselves a challenge of inevitable failure and if one were to take a pessimistic view of the safety history of the process industries then this may well be the case. Although this is where Reason[5] brings us and this papers challenge in “Making Sense of Reason”. His “Safety Space” is a natural extension of the resistance-vulnerability continuum introduced in the previous section. It is a boundary within which the current resistance or vulnerability of an individual or an organization is represented. As shown in Figure 1, it is cigar-shaped, with extreme resistance located at the left-hand end and extreme vulnerability at the right-hand end. The shape acknowledges that most people or organizations will occupy some intermediate point within this space.

An organization's position within the safety space is determined by the quality of the processes used to combat its operational hazards. In other words, its location on the resistance-vulnerability dimension will be a function of the extent and integrity of its defences at anyone point in time.

However, here is no such thing as absolute safety, human fallibility, latent conditions and the possibility of chance conjunctions of these accident-producing factors continue to exist, even the most intrinsically resistant organizations-those at the extreme left-hand end- can still have accidents. By the same token, 'lucky' but unsafe organizations at the extreme right-hand end of the space can still escape accidents for quite long periods of time.

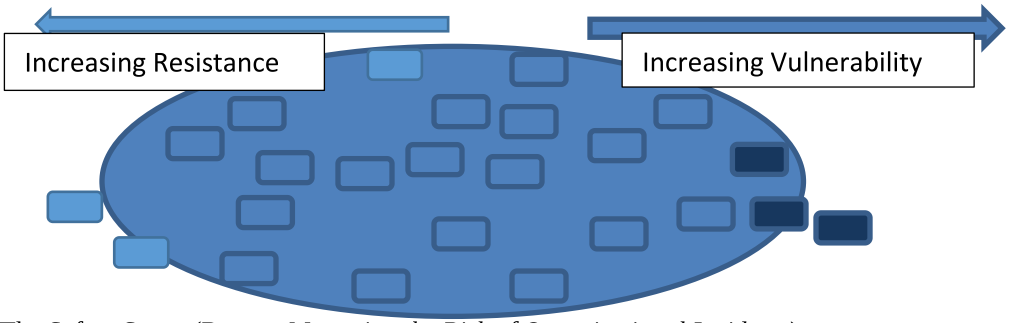

Fig 1: The Safety Space (Reason *Managing the Risk of Organizational Incidents*)

“The key to navigating the safety space lies in appreciating what is manageable and what is not. Many organizations treat safety management as a negative production process, they set reduced negative outcome targets for the coming accounting period (e.g., 'Next year we'll reduce our lost-time accidents by half'), yet accidents by their nature, are not directly controllable, so much of their causal variance lies outside the organization's sphere of influence. The organisation can only defend against hazards; it cannot remove or avoid them and still stay in business. Similarly, an organization can only strive to minimize unsafe acts, it cannot eliminate them altogether, and figure 2 demonstrates some of the high level factors that need to be in place.”

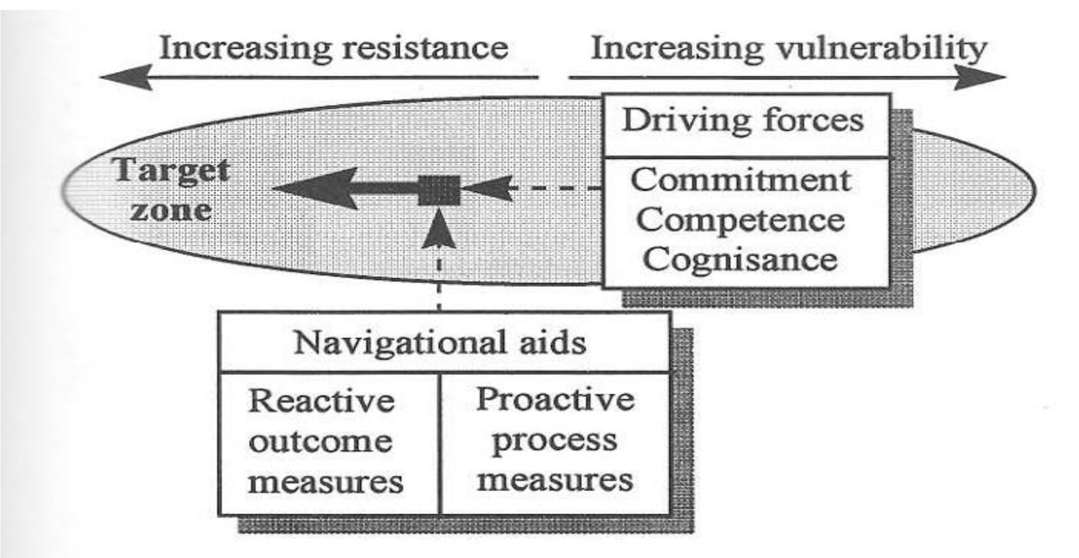

Fig 2: A summary of the principal factors involved in navigating the “Safety Space” with The Driving Forces and the Navigational Aids that together comprise the safety information system (Reason *Managing the Risk of Organizational Incidents*)

This is where the sense of matching our studies and the link to Safety Competency where reports spanning 40 years highlight this common factor amongst many others from our Equation of State:

Date	Event Name
1974	Flixborough
1979	3 Mile Island
1984	Bhopal,
1986	Chernobyl
1998	Piper Alpha
	Longford, Australia
2005	Texas City Buncefield
2010	Deep Water Horizon/Mocondo Dupont Belle Tesoro Refinery
2015	ExxonMobil Torrance, CA
	Tianjin, China

This analysis is supported by Baybutt's "Insights into process safety incidents from an analysis of CSB Investigations" of 64 incidents [8].where he too sees lack of competence arising with regular frequency.

Conclusion

Effective safety management is more like a long-term fitness programme than negative production. Rather than struggling vainly to exercise direct control over incidents and accidents, managers should regularly measure and improve those processes--design, hardware, training, procedures, maintenance, planning, budgeting, communication, goal conflicts, and the like-that are known to be implicated in the occurrence of organizational accidents. These are the manageable processes determining a system's safety health. They are, in any case, the processes that managers are hired to manage; safety management is not an add-on, but an essential part of the system's core business.

Perhaps safety indictors need brought into the management world, where there is no room for "loss time statistics", "leading/lagging indicators", or current position on the "Heinrich's Safety Triangle/Dashboard" and more about:

- Did the work force feel safe at work today?
- What did we do safely today to make the business more secure?
- What marginal gains have we developed today to make us all safer?

These are perhaps 3 from many indicators to be used by managers who normally show concern about the viability of their business by asking about Quality (throughput) & Financial (Cash at bank) indicators.

However, there is a challenge in this view and in addressing "why", it is suggested here that the concept of competence or the lack of it is the problem.

In his review of “Texas City Refinery Explosion: Lessons Learned”, Mogford [6] mentions five underlying causes, all management responsibilities and two in particular are linked to the theme of this paper:

> “Secondly, process safety, operations performance and systematic risk reduction priorities had not been set nor consistently reinforced by management. Safety lessons from other parts of BP were not acted on.
>
> And finally, poor performance management and vertical communication in the refinery meant there was no adequate early warning system of problems and no independent means of understanding the deteriorating standards in the plant through thorough audit of the organisation.”

This is reinforced in the Baker [7] commission report for BP,

> **“Recommendation #3**
> **– process safety knowledge and expertise**
> BP should develop and implement a system to ensure that its executive management, its refining line management above the refinery level, and all U.S. refining personnel, including managers, supervisors, workers, and contractors, possess an appropriate level of process safety knowledge and expertise.”

BP and many other companies have done much in progressing this idea, yet CCPS’s *Guidelines for Auditing Process Safety Management Systems* (2nd edition 2011) places “Training and Performance Assurance” at p547 out of 835, and this really returns to the start of this paper, if the senior management don’t understand

The Process Safety First Equation of State;

Safety Practice (SP) =
F (Materials of Construction (M_c), Property of Materials (P_m), Reaction Kinetics (R_k), Effect of Fires & Explosions (E_{fe})),

Just understanding Cash Flow, Six Sigma, Coaching & Leadership and all the other chapters of *“How to be an Even Better Manager: A Complete A-Z of Proven Techniques and Essential Skills”* or some other book of that ilk, is not being a manager and the anthology of Process safety events presented in this paper will continue.

References

[1] Dickson B.R: Making Sense of Reason: A review of the message James Reason put forward for a re-think of Safety Management Principles, AIChE,11th Global Congress on Process Safety Proceedings, 2015

[2] Dekker Sidney: Drift into Failure Ashgate Publishing 2011

[3] Perrow Charles: Normal Accidents: Living with High risk Technologies, Basic Books, 1984

[4] Weick Karl quoted in P.J. Frost et al.: Reframing Organizations Sage 1991

[5] Reason James: Managing the Risk of Organizational Incidents, Ashgate Publishing, 1997

[6] Mogford J: The Texas City Refinery Explosion: The Lessons Learned**,** AIChE,2nd Global Congress on Process Safety Proceedings, 2006

[7] Baker J: BP US Refineries Independent Safety Review Panel Report, 2007

[8] Baybutt P: Insights into process safety incidents from an analysis of CSB Investigations, *Journal Of Loss Prevention In The Process Industries*, JLPP 3258, 2016